5 - Source Configuration

(Required for Director/Logging/Database Reporting/Event Paging)

SOURCE ENTRY MENU

This section establishes the NetRanger's names and IDs and IP Routing Addresses for the sources of NetRanger Events. Each entry contains the following five fields:

1 - **Organization Name**
2 - **Organization ID**
3 - **Host Name**
4 - **Host ID**
5 - **IP Address to route through**

Org Name	Org ID	Host Name	Host ID	via IP Address

IP address to route through—This is the IP Address of the closest NetRanger Postoffice that can route NetRanger postoffice packets to the destination.

6 - Destination Configuration

(Required for NSX/Director)

DESTINATION ENTRY MENU

This section establishes the NetRanger's names and IDs, IP Routing Addresses, Destination Services, and Event Logging Levels for the destinations of NetRanger Events. Each entry has the following seven fields:

1 - **Organization Name**
2 - **Organization ID**
3 - **Host Name**
4 - **Host ID**
5 - **via IP Address**
6 - **Service**
7 - **Level**

Org Name	Org ID	Host Name	Host ID	via IP Address	Service	Level

IP Address to route through—This is the IP address of the closest NetRanger postoffice that can route NetRanger postoffice packets to the Source.

Service—This is the destination's NetRanger Service.

Level—This is the lowest level Alarm/Event that should be sent to the destination service.

7 - Postoffice Router Configuration

(Required for Postoffice Routing)

ROUTER ENTRY MENU

This section defines the NetRanger's names, Ids, and IP Routing Addresses for remote NetRanger nodes. Each entry has the following five fields:

1 - **Organization Name**
2 - **Organization ID**
3 - **Host Name**
4 - **Host ID**
5 - **IP address to route through**

Org Name	Org ID	Host Name	Host ID	via IP Address

IP Address to route through—This is the IP Address of the closest NetRanger postoffice that can route NetRanger postoffice packets to the Remote NetRanger node.

8 - Sleeve Configuration

(Optional for NSX)

SLEEVED NETWORK ENTRY MENU

This section establishes the Remote Organization ID, Remote IP Routing Addresses, and Remote Network Netmasks for Sleeved Networks. Each entry has the following three fields

1 - **Sleeve Remote Org ID**

2 - **Sleeve Remote IP Address**

3 - **Sleeve Remote Netmask**

Sleeve Remote Org ID	Sleeve Remote IP Address	Sleeve Remote Netmask

Sleeve Remote Org ID— his is the Organization ID for the remote end of the sleeve.

Sleeve Remote IP Address—This is the IP address for the remote end of the sleeve.

Sleeve Remote Netmask—This is the subnet netmask for the remote end of the sleeve.

9 - Clear Temporary Configuration Files

This menu item prompts you to insure that you want to clear the temporary configuration files for the NetRanger software.

```
Are you sure you want to CLEAR the Temporary Configuration files? (y/n)>
```

Answer yes to clear and reinitialize the temporary NetRanger configuration files in /usr/nr/etc/wgc and the temporary BorderGuard configuration files in /usr/nr/etc/nsc to their default values.

10 - Generate Temporary Configuration Files

This menu item prompts you to insure that you want to generate the temporary configuration files for the NetRanger software.

```
Are you sure you want to GENERATE the Temporary Configuration files? (y/n)>
```

Answer yes to write the temporary NetRanger configuration files to /usr/nr/etc/wgc and the temporary BorderGuard configuration files to /usr/nr/etc/nsc.

NOTE

You should review the temporary NetRanger configuration files located in the /usr/nr/etc/wgc directory and the BorderGuard configuration files located in the /usr/nr/etc/nsc directory after nrconfig has generated the temporary configuration data. The temporary NetRanger configuration files **must** be committed to /usr/nr/etc (/tmp for temporary BorderGuard configuration files) after review or after any manual changes. The BorderGuard files must then be loaded onto the NSG BorderGuard.

11 - Edit/Review Temporary Configuration Files

This menu item starts a vi edit on the temporary NetRanger configuration files in /usr/nr/etc/wgc and the temporary BorderGuard configuration files to /usr/nr/etc/nsc.

12 - Review Temporary Configuration Files

This menu item starts a "more" command on the temporary NetRanger configuration files in /usr/nr/etc/wgc and the temporary BorderGuard configuration files in /usr/nr/etc/nsc.

13 - Commit Temporary Configuration Files

This menu item prompts you to insure that you want to commit the temporary configuration files for the NetRanger software to the NetRanger Configuration File Directory.

```
Are you sure you want to COMMIT the Temporary Configuration files to the
NetRanger Configuration File Directory '/usr/nr/etc' and to the BorderGuard
Configuration File Directory '/tmp'? (y/n)>
```

Answer yes to write the configuration temporary NetRanger configuration files to the /usr/nr/etc directory.

NOTE
This overwrites working NetRanger configuration files.

Enter - EXIT

To exit the NetRanger Configuration program, simply hit "Enter" at the menu prompt. This menu item prompts you to insure that you are ready to exit the configuration program.

```
Are you sure you want to EXIT? (y/n)>
```

Answer yes to exit the configuration program.

NOTE
You can exit and restart the NetRanger Configuration program without losing any of the configuration information you have input.

NetRanger configuration is complete.

NOTE
The NetRanger processes **must** be restarted using /usr/nr/bin/nrhup before the committed NetRanger configuration file will take effect.

IV Operating NetRanger

Working With the Director and the NSX

The NetRanger Director is the Graphical User Interface (GUI) for the NetRanger system. The NetRanger Director (also called "the Director") has four main functions:

- provides a graphical, intuitive display of information pertaining to network security violations in real time;
- displays a hierarchical map of the remote NetRanger software and hardware (the Sensor processes and the NSX hardware, for example) that send security notifications to the Director;
- provides utilities for configuration of the remote NetRanger applications; and
- provides utilities to query the database of historical security events.

The Director uses popular network management platforms like HP OpenView and IBM NetView for AIX to display network security information. As a result of this integration, network management personnel do not have to learn multiple-user interface applications and paradigms to perform different network management tasks.

When a process on a remote NSX machine detects a security violation, a notification (called an "event") is sent from the NSX machine to the Director machine. The Director ensures that the machine and application that generated the event are represented on the graphical map, and then, if the event's severity level exceeds a user-definable threshold, the Director creates an Alarm icon on the map. The color of the Alarm icon is based on the severity of the event. The Application and Machine icons also change color, so it is easy to determine at a glance which machine detected the problem. With a few mouse clicks, details about the Alarm (source and destination IP address, for example) can be displayed. Location functions can be used to locate Alarms with specific properties.

Once an Alarm is diagnosed and addressed, the user can delete the Alarm icon from the user interface. The Application and Machine icons revert to their previous state.

Architecture

The NetRanger Director is not a single computer program, but is rather a *set* of applications and background processes that work with a network management platform. The diagram below illustrates the data flow between the processes in NetRanger.

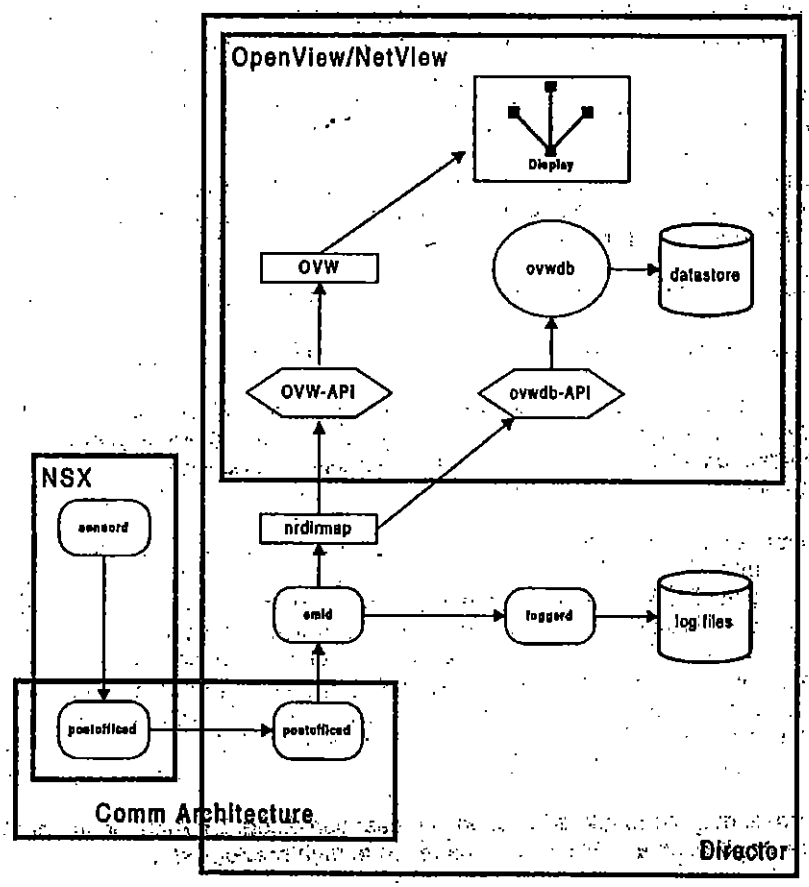

Figure IV-1: The NetRanger Director Architecture

In the diagram above, ovals represent background processes, squares represent foreground applications, cylinders represent datastores, hexagons represent APIs, and lines represent the flow of event data. Note that *ovw* and *ovwdb* are part of OpenView/NetView, *nrdirmap*, *smid*, and *loggerd* are part of the Director, and *sensord* is part of the NSX. Also note that the NSX and the Director both contain *postofficed* processes.

When the *sensord* process detects activity of interest, it generates an event that is sent via the *postofficed* daemons to the *smid* daemon on the Director machine. The *smid* daemon passes the event information to the *loggerd* daemon, which logs the information, and to *nrdirmap*.

nrdirmap looks at the severity level of the event. If the event severity exceeds a user-specified level, then *nrdirmap* tells *ovw* to draw an alarm icon. *nrdirmap* also tells *ovwdb* to create an alarm database object in the OpenView/NetView datastore.

Basic Director Functions

Starting the Director

The Director consists of three separate subsystems:

- The NetRanger background processes
- The network management platform background processes
- The network management platform user interface

NOTE
These subsystems should be started in the order listed above in order to ensure proper operation of the Director.

Starting the NetRanger Background Processes

The NetRanger background processes are configured to start automatically when the machine is rebooted, so in most cases, you will not need to manually start these processes.

In the event that you must start them manually, follow these steps:

1. **Log in as someone in the group `netrangr`, and then type**

   `nrstart`

2. **If the executable is not found, then either type the fully qualified name**

   `(/usr/nr/bin/nrstart)`

   or put `/usr/nr/bin` in your path.

Starting the Network Management Background Processes

Like the NetRanger background processes, the network management platform background processes are configured to start automatically when the machine is rebooted, so in most cases, you will not need to manually start these processes.

In the event that you must start them manually, follow these steps:

1. **log in as `root` and then type:**

   `ovstart`

   If the executable is not found, then the subdirectory that includes the network management binaries is probably not in your path (the location for OpenView binaries is `$OV_BIN`, and the location for NetView binaries is `/usr/OV/bin`). Consult your network management documentation if you have difficulty starting the network management background processes.

Starting the Network Management User Interface

To start the Director's network management user interface, follow these steps:

1. **If you use HP OpenView, log in as a user that belongs to the group `netrangr` and then type:**

   ```
   ovw &
   ```

   If you use IBM NetView for AIX, log in as a user that belongs to the group `netrangr` and then type:

   ```
   nv6000
   ```

NOTE
The *nrdirmap* program will start automatically when you bring up the network management user interface. You will never have to manually start *nrdirmap*.

Stopping the Director

To stop the Director, stop the subsystems in the *opposite* order in which they were started.

Stopping the Network Management User Interface

1. **If you use HP OpenView, select the menu option**

   ```
   Map..Exit
   ```

2. **If you use IBM NetView for AIX, select the menu option**

   ```
   File..Exit
   ```

Usually, you will only want to close the user interface. In most circumstances, you will not want to close the background processes. If you do want to close the background process, follow the steps below.

1. **Log in as user root and then type**

   ```
   ovstop
   ```

   If the executable is not found, then the subdirectory that includes the network management binaries is probably not in your path (the location for OpenView binaries is `$OV_BIN`, and the location for NetView binaries is `/usr/OV/bin`). Consult your network management documentation if you have difficulty starting the network management background processes.

Stopping the NetRanger Background Processes

To stop the NetRanger background processes, follow these steps:

1. **Log in as someone in the group `netrangr` and then type:**

   ```
   nrstop
   ```


2. **If the executable is not found, then either type the fully qualified name**

   `(/usr/nr/bin/nrstop)`

   or put `/usr/nr/bin` **in your path.**

Checking the Status of the Director Processes

To check the status of all Director processes, follow these steps:

1. **To ensure that the network management background processes are running correctly, type**

   `ovstatus`

2. **To ensure that the NetRanger background processes are running correctly, type**

   `nrstatus`

   If either of these executables cannot be found, check your path.

Understanding the Director's Submap Hierarchy:

When you double-click on a symbol, a submap is opened. This submap could have many symbols on it, and these symbols could be double-clicked to reveal more submaps, each with many symbols. This set of descending submaps can be thought of as an upside-down tree with more and more branches. This upside-down tree structure of submaps and symbols is called the "submap hierarchy".

Traversing the submap hierarchy that nrdirmap creates is easy once you understand the following structure:

This type of submap...	can contain these symbols:
Root	Collection
Collection	Machines (NSX and Director)
	Collections
	Connections
Machine	Applications
Application	Alarms
	Alarm Sets

NOTE

Note that Connections and Alarms do not have submaps. They represent the "leaves" in the submap tree.

Figure IV-2 illustrates the Root submap. It is the highest level submap in the hierarchy. The root submap has no "parent submap". On the root submap, there should be a symbol representing a Collection of machines.

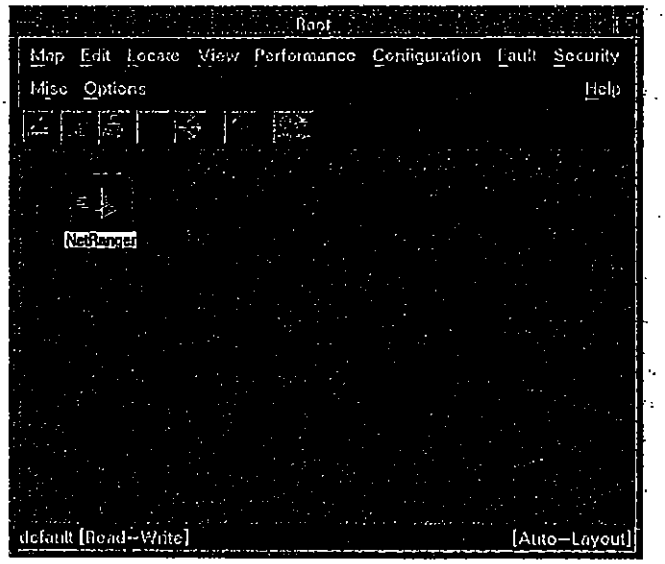

Figure IV-2: The NetRanger Director Submap

When you double-click on a Collection symbol like the one shown in Figure IV-2 , a Collection submap is displayed. A Collection submap can have NSX Machines, the Director Machine, other Collection symbols, and Connections between Machines. The Collection submap shown on the following page only contains a Director machine symbol.

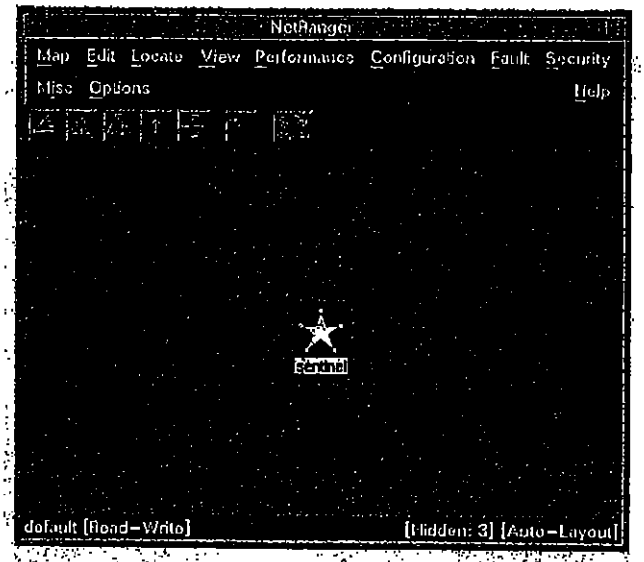

Figure IV-3: A Collection Submap

When you double-click on a Machine symbol, a Machine submap is displayed. A Machine submap contains symbols that represent the different applications running on the machine.

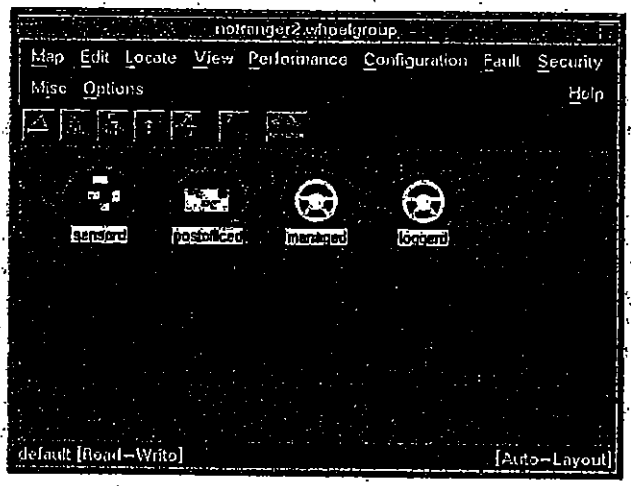

Figure IV-4: A Machine Submap

When you double-click on an Application symbol, an Application submap is displayed. An application submap contains alarms that that application had generated. For instance, if the *sensord* application for a machine generates an event and sends it to the Director, the Director will draw an alarm icon on the submap belonging to that machine's application.

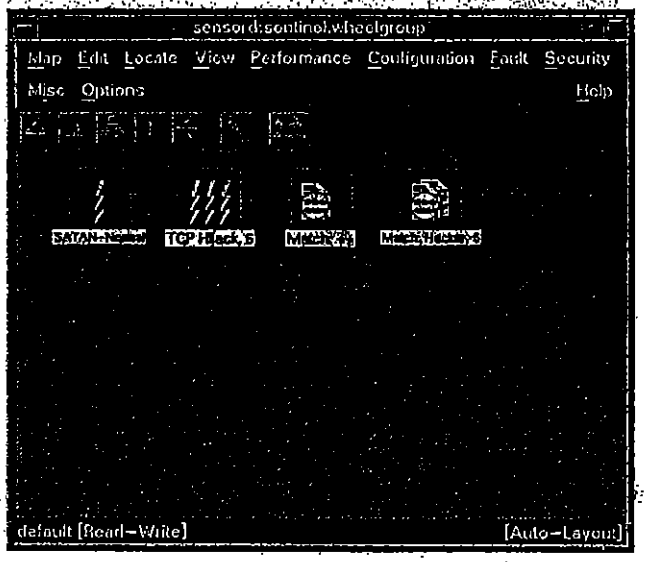

Figure IV-5: An Application Submap

For most alarms, the label under the alarm symbol will match the alarm's "Alarm Name" attribute. For instance, an alarm with the Alarm Name "Net Sweep" will have a "Net Sweep" symbol label.

Alarms with the name "String Match" and "Sec Violation" (Security Violation) will have the their symbol labels taken from the "Alarm Details" attribute. This is because there are many types of Security Violations, and there are an infinite number of potential string matches, so for these two alarm types the Alarm Name itself is not specific enough. For Security Violation alarms, the label will match the name of the specific violation, and for String Matches, the label will be the string that was detected.

Application submaps can also contain a special Alarm symbol called an "Alarm Set". An Alarm Set is created when multiple alarms are received that are identical in all respects *except for* timestamp *and* sequence number. For example, if you get 20 string match alarms with the same attributes (source and destination address, source and destination port, etc.), then the 20 alarms will be represented by a single Alarm Set symbol.

Alarm Sets can be differentiated from Alarms in two ways. First, the end of an Alarm Set symbol label will have a comma followed by the number of alarms represented by the Set. Second, the Alarm Set symbol type is slightly different from an Alarm symbol type. An Intrusion Alarm icon has one lightening bolt and an Intrusion Alarm Set has multiple lightening bolts. A String Match Alarm icon has one sheet of paper behind a magnifying glass and a String Match Alarm Set icon has multiple sheets of paper behind a magnifying glass.

If an Application has generated no Alarms, then a special Alarm called an "OkAlarm" will be displayed that indicates that the Application has no unresolved Alarms.

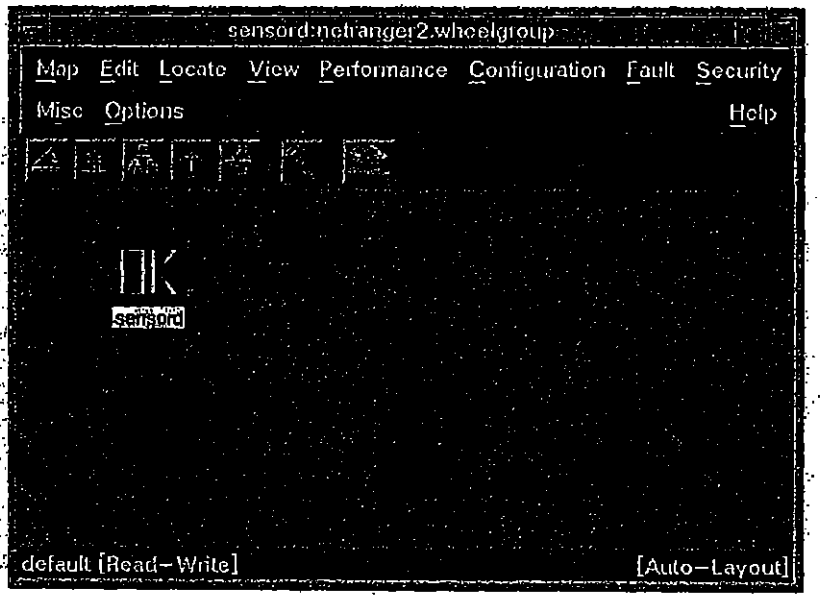

Figure IV-6: An OkAlarm

Adding Entities

In general, there are four types of icon symbols: alarms (which include Alarm Sets and OK Alarms), applications, machines, and collections.

Alarm symbols, at the bottom of the submap hierarchy, can only be created by the *nrdirmap* application. An alarm symbol is created whenever an event that exceeds a user-defined threshold is received. There is no way for a user to manually create an alarm symbol.

There are two ways that Application and Machine symbols can be created. First, if an application or host from which an event emanates is not already represented in the map, then *nrdirmap* will create the symbols for you.

If you do not want to wait until an alarm comes in to have a machine or an application represented in a map, you can add the symbols manually. The next two sections describe how to add machines and applications.

Manually Adding an NSX Machine Symbol

To manually add an NSX machine symbol, follow these steps:

1. **Double-click on a Collection symbol to open the Collection submap (the symbol on the root submap labeled "NetRanger" is a Collection symbol). Machines can only be added to Collection submaps! Do not try to add a Machine to a non-Collection submap.**
2. **Select the** Edit→Add Object **menu function. The** Add Object Palette **will appear.**
3. **Click on the** Net Device **icon. Several icons will appear in the bottom of the palette (see picture below).**

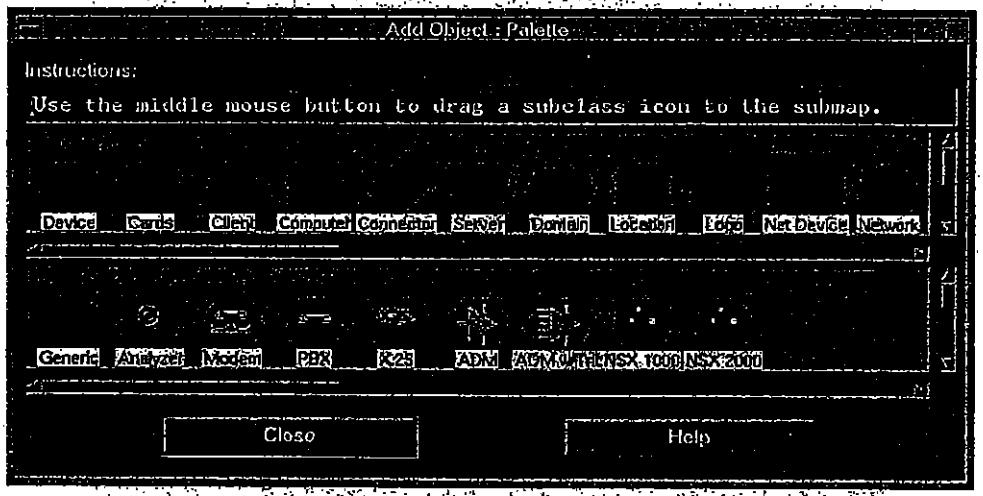

Figure IV-7: The Add Object Palette

4. **Position the mouse pointer over the** NSX 2000 **icon, press and hold the** middle **mouse button, and drag the** NSX 2000 **icon to the collection submap. An** Add Object **window should appear.**
5. **Select** NetRanger/Director **from the list, and press the** Set Object Attributes **button.**

6. In the hostname field, enter the name of the NSX machine exactly as you entered it in the /usr/nr/etc/hosts file.
7. Press the Verify button. If you entered the hostname correctly, NetRanger/Director will populate the Organization and Host Id fields for you.
8. Once the hostname, Organization ID, and Host ID are correct, press OK.
9. Press the Set Selection Name button. Choose the selection name from the list and then press OK in the Selection Name window. Press the OK button in the Add Object Window.

Manually Adding an Application Symbol

1. Double-click on the NSX Machine to which you wish to add the application. Applications can only be added to Machine submaps! Do not try to add an Application to a non-machine submap!
2. If the Add Object Palette is not already displayed, bring it up by selecting the Edit→Add Object menu function.
3. From the Add Object:Palette, click on the WGC Application icon. Several icons should appear in the bottom of the window.
4. Using the same technique described above, drag the application icon to the NSX submap.
5. Select NetRanger Director from the list, and press the Set Object Attributes button.
6. All fields will be populated for you. Press OK.
7. Press the Set Selection Name button. Choose the selection name from the list and then press OK in the Selection Name window. Press the OK button in the Add Object Window. You should see the Application icon turn green, because a green OkAlarm will be created automatically in the submap of the Application you just added.

Manually adding the Director Machine

Normally, you will not need to manually add the Director Machine. The Director Machine symbol is added for you automatically when nrdirmap comes up the first time. However, it is possible to manually delete the Director Machine, and you may want to manually add the Director Machine back to the map at a later time. Also, if you ever change the Organization ID or Host ID of the Director, then you must delete the Director Machine symbol and add it back with the correct IDs.

Please note that only one Director Machine can be represented at a time. In a future release, this restriction may be eased, but for this release, you can only have one Director icon on a map.

The procedure for adding a Director Machine symbol is almost identical to the procedure for adding an NSX Machine symbol. The only differences are as follows:

- From the Object Palette, instead of clicking on the "Net Device" symbol class, click on the "Computer" symbol class.
- Instead of dragging an NSX Machine symbol from the palette, drag the Director Machine icon.
- When you press the **Set Object Attributes** button, you shouldn't have to enter any data. Unless configuration files (like /usr/nr/etc/hosts) are missing or incorrect on your Director Machine, nrdirmap should be able to fill in this information for you.

Manually Adding an NSX Collection

The **Top-Level NSX Collection** (the entity that appears on the Root submap labeled **NetRanger**) is created for you. This is the only Collection that can appear on the root submap. Do *not* try to create additional Collections on the root submap.

NSX Collections are used to customize, or "partition," the map. NSX Collections are good tools to use to group machines into logical units. See the section of this guide called *How to Customize a Map* for more information about specific uses of NSX Collections.

Follow these steps to add an NSX Collection:

1. **Double-click on the NSX Collection's submap to which you want to add the new NSX Collection.** NSX Collections can only be added to NSX Collection submaps! **Do not try to add an NSX Collection to a non-NSX Collection submap!**
2. **If the** Add Object Palette **is not already displayed, bring it up by selecting the** Edit→Add Object **menu function.**
3. **From the** Add Object:Palette, **click on the** Location **icon. Several icons will appear in the bottom of the window.**
4. **Using the same technique described above, drag the symbol that has the WheelGroup Logo to the NSX submap.**
5. **Select** NetRanger Director **from the list, and press the** Set Object Attributes **button.**
6. **In the** NSX Collection Name **field, enter the name of the NSX Collection you just moved to the submap. This name can be any unique string. For example, "New York," "Building 162," or "10.1.1 Machines" would be legitimate NSX Collection Names.**
7. **Press the** Verify **button.**
8. **Press** OK.
9. **Press the** Set Selection Name **button. Choose the selection name from the list and then press OK in the Selection Name window. Press the** OK **button in the Add Object Window.**

Modifying and Viewing Entity Attributes

Once an entity has been created (either by a user or by *prdirmap*), it is often helpful to view a listing of the entity's attributes. Some attributes can be edited by the user (for instance, a machine's Point of Contact), and other attributes are read-only (for instance, an alarm's Date). OpenView/NetView provide visual indication of which fields are changeable and which are not.

To display an entity's attributes, select the entity with the mouse pointer, and then select the menu function **Edit→Describe/Modify→Object**. You can also select the entity and type *ctrl-o*, and you can also put the mouse pointer over the icon, press the right mouse button, and select Describe→Modify Object. A pop-up window will appear. Select **NetRanger Director** from the list of applications, and then press the **Configure** button.

Different entities have different attributes, so each entity will be discussed separately.

NSX Collection Attributes

The NSX Collection Name is the single attribute of a NSX Collection. If you change the Name, and then press **OK** on the appropriate screens, the NSX Collection's symbol label and submap name will change to reflect the new name.

Machine Attributes

Machines have four attributes: **Organization ID, Host ID, Hostname,** and **Point Of Contact.** The hostname and point of contact are editable, but the **Org ID** and **Host ID** are not. If you need to change an Org or Host ID, the best thing to do is to delete the machine and then re-add the machine with the correct IDs. If the hostname is changed, the Machine's symbol label will be the part of the hostname up to the first dot ("."), and the submap name will be the entire hostname.

If you want to store more information about the Point of Contact than the single field will contain, there are two things you can do. First, you can use the **Object Comments** field to store the additional point of contact information. Second, you could put the point of contact information in a separate trouble-ticketing system.

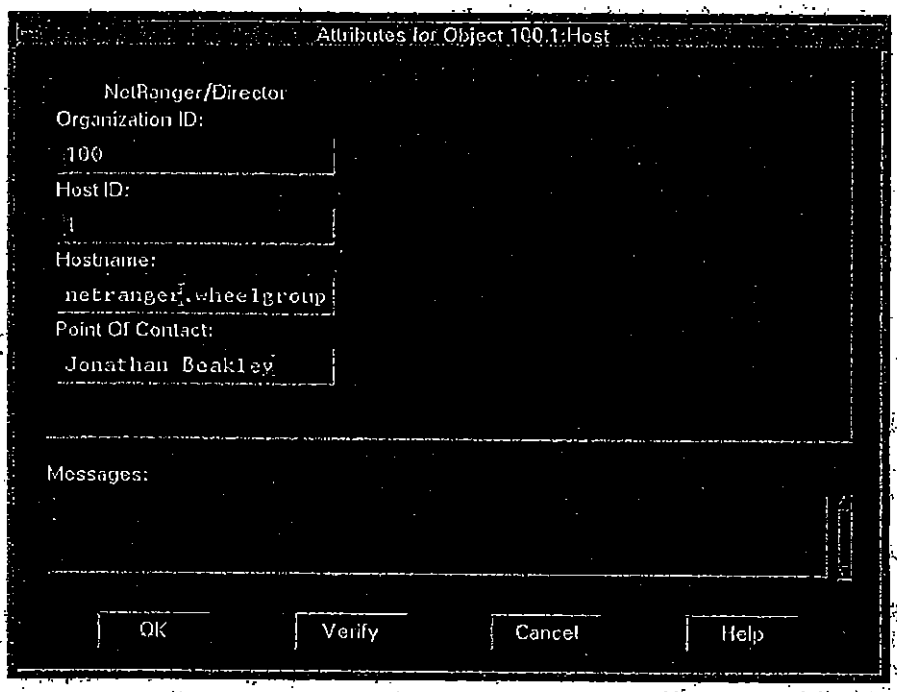

Figure IV-8: Object Attributes Window

Application Attributes

Machines have six attributes: **Application Name, Minimum Marginal Status Severity, Minimum Critical Status Severity, Alarm Consolidation Threshold, Organization ID, Host ID,** and **Application ID.** The application name, status severity fields, and consolidation threshold are editable, but the ID fields are not. If you need to change an ID, delete the application and then re-add it with the correct IDs. If the application name is changed, the Application's symbol label will change to match the new application name, and the Application's submap name will reflect the new name, too (the format for the Application submap name is **<hostname>:<application name>**).

The **Minimum Marginal Status Severity** describes the lowest severity status an event can have before a marginal (yellow) alarm is created to represent that event. For example, if the minimum marginal status severity is 3, and a severity 2 alarm comes in, then no alarm entity will be created.

NOTE

The higher the severity level, the more severe the alarm. Currently, severity 6 is the highest severity level assigned by the *sensord* daemon.

The **Minimum Critical Status Severity** describes the lowest severity an event can have before a critical (red) alarm is created to represent that event. For example, if the minimum critical status severity is 3, and a severity 4 alarm comes in, then a critical alarm will be created.

NOTE

If you change a status severity value, only events generated **after the change** will be affected. If you increase a threshold severity level from 2 to 3, *nrdirmap* will not remove any existing level 2 alarms from the application's submap. Also, if you decrease a threshold severity level from 3 to 2, nrdirmap will not check historical log files and create alarm icons for severity level 2s that may have occurred in the past. Note that Connections and Alarms do not have submaps.

The **Alarm Consolidation Threshold** describes how many identical alarms must be received before the alarms are replaced by a single "Alarm Set" icon. By default, if two or more alarms are received that are alike in all respects except for timestamp and sequence number, nrdirmap will represent these alarms with a single "Alarm Set" icon. This prevents the screen from being cluttered when many similar alarms are received.

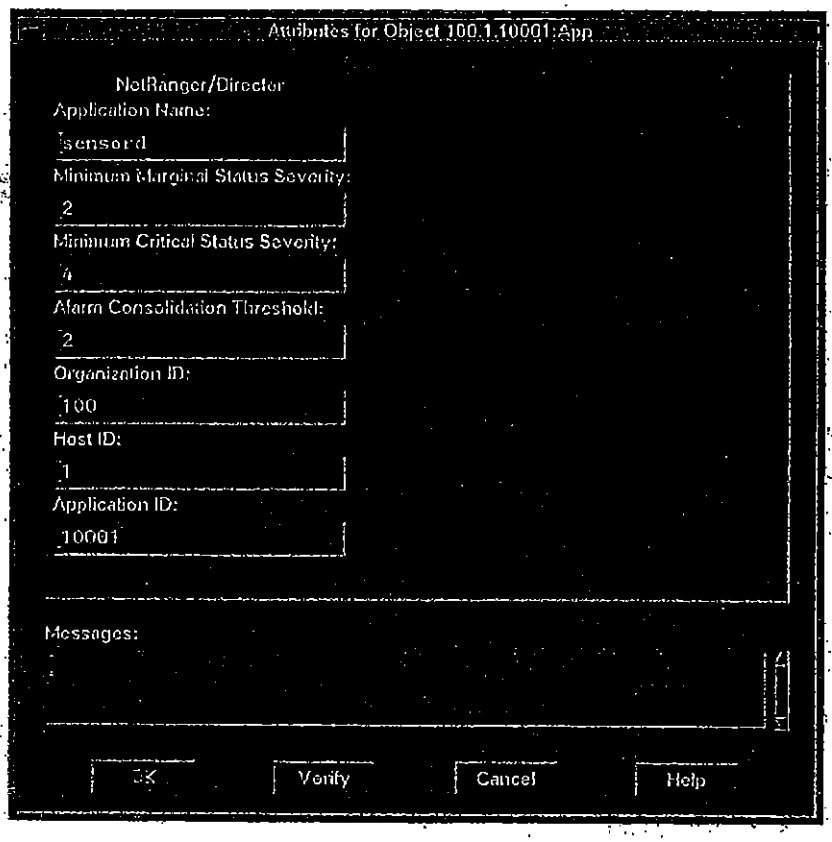

Figure IV-9: sensord Attribute Information

Alarm Attributes

Alarms have many attributes: **Name, Severity, Source Port, Destination Port, Source Address, Destination Address, Router Address, Date, Is Source Address Protected, Is Destination Address Protected, Details, Signature ID, Subsignature ID, Organization ID, Host ID, Application ID, Instance ID.** All alarm attributes are read-only.

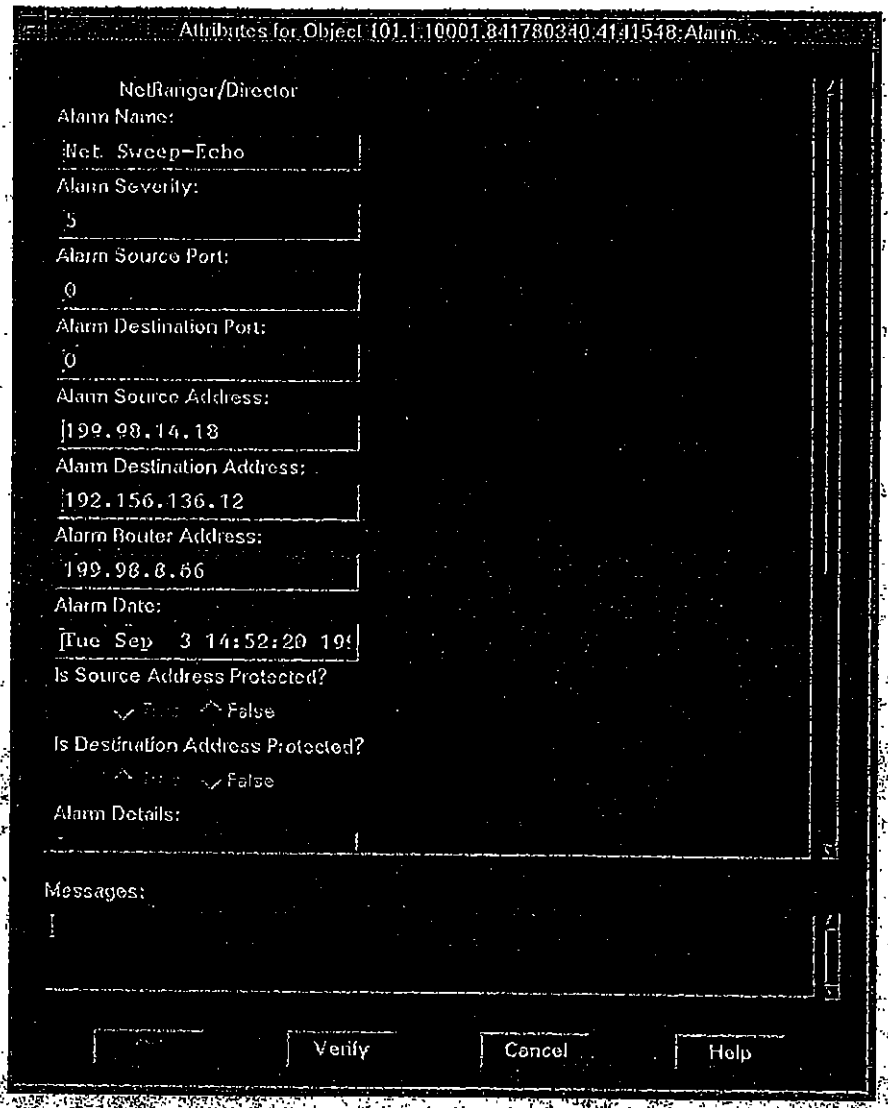

Figure IV-10: Alarm Event Attributes

By default, when two or more alarms are received that are alike in all respects except for timestamp and sequence number, nrdirmap will represent these alarms with a single "Alarm Set" icon. The attributes of an Alarm Set are almost the same as the normal Alarm. The Alarm Set does not have a timestamp and sequence number. Instead, it has an Alarm Count, Date of First Alarm in Set, and Date of Last Alarm in Set.

Once an Alarm Set is created, if additional matching alarms are received, the Alarm Count is incremented, and the Alarm Date(s) are changed if applicable. Note that the symbol label for an Alarm Set is similar to an Alarm, except that after the Alarm Name, the Alarm Count is given.

The special **OkAlarm** that indicates that an application has no unresolved alarms has only four attributes: **Date, Organization ID, Host ID,** and **Application ID.** All these fields are read-only. The Date field specifies the time at which the **OkAlarm** was created. This gives a lower boundary to the last time that the application in question detected an attack.

Deleting Entities

When you want to remove a symbol (and its corresponding database object), you must select the symbol and then choose the **Edit→Delete Object→From *All* Submaps** menu option. The most common usage of the delete function is deleting an alarm symbol once the potential hacking attempt has been diagnosed and resolved.

There are rules governing the deletion of symbols that help prevent the accidental removal of alarms and other symbols. One general rule to remember is this:

NOTE

Applications and Machines can NOT be deleted until ALL of their alarms have been deleted.

This forces the user to go into the submap containing the alarms and specify that it is OK to delete the alarms. This helps prevent a hacking attempt from going unnoticed.

Once an application or host has had all of its alarms resolved (and deleted) you are free to delete the application or machine.

NOTE

If you delete an application or machine, and then an event is received for that machine, the machine will be redrawn on the map. In a case like this, it might be better to *hide* the machine (see the description of the Hide function, below).

Because it would be very easy to accidentally delete large groups of machines, non-empty Collections cannot be deleted. If you have a Collection that contains many machines, and you want to delete the Collection, you must first go into the Collection submap and delete all of the machines (and of course, the machines must have their alarms deleted before the machines can be deleted). Once you have emptied the collection submap, you can then delete the Collection.

NOTE

Never use the Delete Submap function! *nrdirmap* does *not* support this function. Always use the **Delete Object** function to delete entities!

How to Partition a Map

NSX Collection entities can be used to customize, or "partition" a map. If the number of NSX machines you are monitoring is too great to represent on a single submap (for instance, the Top-Level NSX Collection submap), you can create additional Collections, and then add Machine icons to those Collection submaps. This allows you to create a hierarchical grouping of machines.

For example, if you had 25 NSX machines in Los Angeles, and 35 machines in New York, you could create an "LA Collection" entity and a "NY NSX" Collection entity. You could then add the NY NSX Machines to the NY Collection, and then add the LA NSX Machinesto the LA Collection. This allows you to have fewer symbols per submap, which makes locating symbols and diagnosing problems faster and easier.

NOTE

To put a machine in a collection, you must use the **Add Object** function. If a machine is already represented on the map, and you want to move the representation (the symbol) from one collection to another, you must delete the machine and then re-add it. ***nrdirmap does not support the "Cut and Paste" functionality!*** Use of the Cut and Paste functionality on *nrdirmap* entities will yield unexpected results. *You must delete a machine and then re-add it to move the machine symbol from one Collection to another.*

Changing Map Configuration Parameters

There are five global Map-level configuration parameters that can be set. To see these parameters select the menu option **Map→Maps→Describe/Modify.** You will then see a pop-up window. On this window, choose the **NetRanger Irector** application, and then press the **Configure** button.

A window with five parameters will appear. You will see the following questions:

1. **Default lowest event severity that generates marginal icon?**
2. **Default lowest event severity that generates critical icon?**
3. **Default Number of Identical Alarms before Icon Consolidation?**
4. **Should nrdirmap be enabled for this map?**
5. **Should new security alarms be shown on the IP Map?**

The answer to the first question specifies the minimum severity an event must have before a marginal (yellow) Alarm is generated. For instance, if you set this value to 2, then if any new applications are created, these applications will have marginal alarms generated for events whose status is two and higher. Of course, if you manually reconfigure the Application symbol to have a new marginal status threshold, then this default value will be overridden.

To use the Show Context function, select one or more Alarm or Alarm Set icon(s), and choose **Security→Show→Context**. An "xnmappmon" window will appear that displays three fields:

- "String Matched"—this field displays the string that was matched. The maximum length of this field is 64 bytes.
- "Context Buffer 1"—this field displays up to 256 bytes of information that was transmitted in a single direction (either from or to the Server) at the time the string match occurred.
- "Context Buffer 2"—this field displays up to 256 bytes of information that was transmitted in the opposite direction (either to or from the Server) at the time the string match occurred.

NOTE

All non-printable ASCII characters are displayed using a "\" character and two hex digits. For example, <ctrl-g>, which has ASCII value "07" in hex, is represented as "\07". The ASCII character "\" itself is represented as "\\".

If there is no context information available for an Alarm, then the "xnmappmon" window will display the following message:

```
Could not find context alarm information for alarm <Alarm Name>.
```

Viewing Event Lists

To view an ASCII list of the latest events that have been generated for a given application or machine, simply select either an Application or a Machine symbol from the map, and then choose the menu option **Security→Show→Current Events**.

This will execute a program that parses the log files in /usr/nr/var, looking for *all* events for the entity selected. Please note that this will include events that may be below the threshold for creating alarms.

Also note that this window is dynamically updated as new events come in. This is why the "hourglass" mouse pointer never goes away. The program does not stop until you press the **Stop** button, because it is always looking for new events.

To stop the search for new events, press the **Stop** button. After you have done this, you can enter new IDs (org/host ID pairs, or org/host/app ID tuples) and restart the search with the **Restart** button. You can also use the various save and print utilities to store the data you have collected.

Press **Stop** and then **Close** to stop the event search and close the window.

The events are displayed with an OpenView/NetView utility called **xnmappmon**. You can change the fonts and layout of this utility by changing the application defaults file for this utility (see your network management platform documentation for details).

Resolving an Alarm's IP Addresses

The **Security→Show→Names** function can be used to find the hostnames of an alarm's source and destination IP addresses. To use this function, select one or more Alarm (or Alarm Set), and select **Security→Show→Names.**

An xnmappmon window will display the hostnames if they can be found. If the IP addresses cannot be resolved, you will see the following message:

```
"*** <Resolver> can't find <IP Address>: Non-existent domain"
```

Determining the Version of a Remote NetRanger Daemon

The Director includes a utility called *nrVersion* that determines the Version of NetRanger code running on a machine. This function is helpful when diagnosing problems or upgrading software. To run nrVersion, simply select one or more Machine or Application symbol, and then choose **Security→Show→Version.**

An "xnmappmon" window will display the version numbers of all NetRanger applications that are selected, and/or the version numbers of all NetRanger applications on any machines that are selected.

If you see the following message

```
Error: Problem sending query to nr.configd
```

then the version of nr.configd that you are using does not support this menu function. You should also ensure that nr.configd is running on the remote machine.

Shunning IP Addresses and Class C IP Networks

The **Security→Shun** functions can be used to manually shun (block) incoming IP traffic. To shun traffic that emanates from an Alarm's Source IP Address, select the Alarm (or Alarm Set), and choose **Security→Shun→Source IP.** To shun traffic that emanates from any IP address within the Class C Network that contains an Alarm's Source IP Address, select the Alarm (or Alarm Set), and select **Security→Shun→Source Net.**

In either case, an xnmappmon window will display the output of the nrexec command that was used to shun the traffic.

Please note that the default timeout value for the nrexec command is 10 seconds, and that the default duration for the shun is 1440 minutes (one day). To extend the duration, to stop the shunning, or to otherwise exercise more granular control, use the **Security→Configure** menu function.

Saving Object Data to a File

Use the **Security→Save To File** function to direct the attributes of one or more objects to a file. This is helpful if you want to e-mail alarm details to someone.

To use this function, select one or more symbols on the map, and then choose **Security→Save To File**. An ASCII file will be created in /usr/nr/tmp. The filename(s) will match the selection name(s) of the object(s) you selected.

This function uses the OpenView "ovobjprint" utility. For more information about ovobjprint, see the ovobjprint man page.

Finding Out About nrdirmap

Use the **Security→About** function to find information about the version of nrdirmap that you are using.

Changing IP Addresses, Hostnames, and NetRanger IDs

If you change the IP characteristics of either a Director or NSX machine, or if you change the NetRanger communication infrastructure characteristics (like hostId, orgId, host name, and organization name), you *must* ensure that the appropriate configuration files have been changed on *all* your NetRanger machines, including the Director machine.

If you change the hostId or organizationId of either an NSX machine or the Director machine, after making the necessary changes to the configuration files, ensure that you use the **Edit→Delete** menu option to delete the machine from the map. After this is done, use the **Edit→Add Object** menu function to add the machine back to the map with the proper Ids. See the sections on adding and deleting objects for more information about these procedures.

If an IP Address is changed, ensure that the /usr/nr/etc/routes, /usr/nr/etc/sensord.conf, and /usr/nr/etc/managed.conf files are changed as necessary. If host or organization names have changed, ensure that the /usr/nr/etc/auths, /usr/nr/etc/destinations, /usr/nr/etc/hosts, /usr/nr/etc/routes, and /usr/nr/etc/smid.conf reflect the new configuration. If host or organization IDs have changed, ensure that the /usr/nr/etc/hosts has changed. All this can be done with the nrconfig utility.

If the IP address or hostname of the network management station must be changed, consult your network management documentation to learn about what configuration changes must be made to your network management platform. On HP systems, it is recommended that you shut down the user interface, stop the OpenView daemons, stop the NetRanger daemons, and then use SAM to reconfigure the IP information. If you are changing the hostname, you should run `/etc/set_parms hostname` to ensure that the Common Desktop Environment is aware of the new hostname. Once this is done, and once any additional OpenView-specific configuration is complete (as specified in the OpenView documentation), it is recommended that you reboot your machine.

Changing Registration Files

All OVw Applications have a configuration file called a Registration File that tells the User Interface (OVw) how to treat the application. On HP systems, registration files are kept in `$OV_REGISTRATION/C`, and on IBM systems, the files are stored in /usr/OV/registration/C.

In general, registration files should not be modified, but there are a few circumstances in which it is helpful to edit registration files. Registration files contain the command that is actually used to launch the OVw Application, so registration files are good places to edit an OVw Application's command-line parameters.

The following table lists nrdirmap's command line parameters:

Opt	Params	Function
-a	<int>	default Alarm consolidation threshold for new maps
-c	<non-zero int>	default Critical value threshold for new maps
-d	<none>	Disable nrdirmap for new maps by default
-f	<none>	force Full synchronization
-m	<non-zero int>	default Marginal value threshold for new maps
-p	<none>	Propagate to IPMap for new maps
-s	<int>	number of Seconds to be idle before sleep
-t	<none>	Tracing enabled

-a, Alarm consolidation threshold

By default, if two or more alarms are received that are alike in all respects except for timestamp and sequence number, nrdirmap will represent these alarms with a single "Alarm Set" icon. This prevents the screen from being cluttered when many similar alarms are received.

An alarm consolidation threshold is configurable for each application object that is represented in the map.

The -a option is used to define a new *default* alarm consolidation threshold. This default value is applied to all application objects that are created *after you change the default value.* For example, if all of the application icons in your map have an alarm consolidation of 2, and then you set the -a option to 5, then whenever a new application is created, the new application will have the threshold of 5. Please note that the -a option will have no effect on *existing* application entities.

The default is 2. A value of 0 means no alarm consolidation. Any integer zero or higher is valid.

-c, Critical value threshold

By default, if nrdirmap receives an event with a severity level of 4 or higher, the symbol that represents that alarm will have "Critical" status. Unless the user specifies otherwise, a symbol with Critical status will be red.

A critical value threshold is configurable for each application object that is represented in the map.

The -c option is used to define a new *default* critical value threshold. This default value is applied to all application objects that are created *after you change the default value.* For example, if all of the application icons in your map have a critical threshold of 4, and then you set the -c option to 3, then whenever a new application is created, the new application will have the threshold of 3. Please note that the -c option will have no effect on *existing* application entities.

-d, Disable nrdirmap by default for new maps

By default, when a new map is created, nrdirmap will be enabled, which means that nrdirmap will display security information on the new map. If you would like for nrdirmap to be disabled for new maps by default, add the "-d" option to the nrdirmap registration file.

See the section in this chapter entitled *Limiting Access to Security Information* for more information about enabling and disabling nrdirmap.

-f, force Full synchronization

By default, when a symbol that exists in multiple maps is deleted from a map, the symbol will not be redrawn on the map when the user interface is stopped and restarted. The idea is that once you delete a symbol from a map, the symbol is deleted permanently. Once a symbol is deleted from *all* maps, the object that the symbol represents is deleted from the object database.

This means that there could be objects in the database that might not be represented as symbols in one or more of your maps (for instance, if you have two maps, and you delete an alarm symbol from one of the maps, the alarm object is still in the database, but there is no symbol for that object in one your maps).

If you ever want to "refresh" a map to ensure that all objects in the database are represented in a map, use the -f option. This will force nrdirmap to represent all objects in the database as symbols on the map you just brought up.

Note that this option should have no effect if you only have one map.

If you have multiple maps, and you want to "recover" a symbol that was accidentally deleted from a map, you can use this option (assuming that the object is still represented as a symbol in another map).

-m, Marginal value threshold

By default, if nrdirmap receives an event with a severity level greater than or equal to 3 and less than the critical threshold value (discussed above), the symbol that represents that alarm will have "Marginal" status. Unless the user specifies otherwise, a symbol with Marginal status will be yellow.

A marginal value threshold is configurable for each application object that is represented in the map.

The -m option is used to define a new *default* marginal value threshold. This default value is applied to all application objects that are created *after you change the default value.* For example, if all of the application icons in your map have a critical threshold of 3, and then you set the -m option to 2, then whenever a new application is created, the new application will have the threshold of 2. Please note that the -m option will have no effect on *existing* application entities.

-p, Propagate to IP Map

This option currently has no effect. This option may be used in a later version of the product.

-s, Seconds to be idle before sleep

By default, if nrdirmap does not receive an alarm or a user interface callback for 5 seconds, it will go to "sleep", and wake up once per second to check for new events. Once a new event is received, it will handle new events as fast as they come in, until 5 seconds pass with no more events. At this point, nrdirmap goes back to sleep.

To change the amount of time in seconds before sleep, use this option. Under normal circumstances, there will be no reason to change this value from the default of 5 seconds.

-t, Tracing enabled

If nrdirmap is malfunctioning, your authorized service representative might instruct you to enable tracing by adding the -t option. After you set this option, it is best to bring down the user interface, and then bring it back up by typing:

```
ovw > /usr/nr/tmp/nrdirmap.out
```

NOTE

This will create a file called nrdirmap.out with information that can be used by a WheelGroup representative to diagnose the problem. Please not that if you do not redirect the trace messages, the messages will go to standard out.

Command-Line Parameter Examples:

1. **To enable tracing, type**

```
Command -Shared -Initial -Restart "nrdirmap -t";
```

2. **To create marginal icons for level 2 alarms and critical icons for level 3 and higher alarms, type**

```
Command -Shared -Initial -Restart "nrdirmap -m 2 -c 3";
```

3. **To enable tracing and to create Alarm Sets once 15 similar alarms are received, type**

```
Command -Shared -Initial -Restart "nrdirmap -t -a 15";
```

Changing the Number of Events Displayed in Event List

When you select a Machine or Application symbol and select the menu option **Security→Show Current Events**, by default the last 100 events associated with that entity are displayed (if less than 100 events are known, then all of the events are displayed). To change the number of events that are displayed, use an editor to modify the nrdirmap file, which is stored in `$OV_REGISTRATION/C` on HP systems and /usr/OV/registration/C on IBM systems.

Replace the "100" with the number of your choice on the line shown in bold.

```
Action show_events  {
        SelectionRule (isWheelGroup && (isMachine ||
isApplication));
        MinSelected  1;
        Command "sh -c 'unset OVwSessionLoc \;
                $OV_BIN/xnmappmon \
                -selectList \" ${OVwSelections} \" \
                -commandTitle \" Show Current Events for \"
\
                -appendSelectList \
                -appendSelectListToTitle \
                -multipleDialogs \
                -headingLine 2 \
                -geometry 900x600 \
                -followOutput \
                -unbuffO \
                -stopSignal 9 \
                -cmd /usr/nr/bin/filterLogByHostApp -l 100'
    ";
    }
```


Changing Symbol, Object, and Submap Characteristics

The OpenView user interface (ovw) provides functions that modify characteristics of symbols (icons) and database objects.

Unfortunately, the user interface is perhaps a bit *too* powerful, in that it allows a user to change data in ways that can confuse the nrdirmap application. This section describes what user modifications are allowed, and which are not.

Object Modifications

Object Modifications are made through the "Modify→Describe Object" menu function.

It is OK to change the "Comments" field, and it is OK to change any attribute field that is editable from the window that is accessed by selecting "NetRanger Director" and pressing the **View/Modify Object Attributes** button. Please note that any changes you make to an object *will apply to all maps*. Remember that symbols are map specific, but database objects are shared among all maps.

You should not edit the Selection Name. The Selection Name field is a field that is used to uniquely identify an object.

Symbol Modifications

Symbol modifications are made through the **Modify→Describe Symbol** menu function.

You can change the "Display Label" setting, and you can change a symbol from "explodable" to "executable".

In general, changing the symbol label itself is not recommended, because nrdirmap has specific algorithms it uses to determine the symbol label, and it will override your label customization when the user interface is stopped and started.

You should not change the "symbol status source" because nrdirmap expects all symbols (except alarm symbols) to have "Compound Status Source". This ensures that an alarm's status is always propagated "upward" in the submap hierarchy. Changing the status source will jeopardize this.

You should not change the symbol type. This will cause "capability fields" in the object database to be changed, and this will affect many different functions—including synchronization and callback communication between nrdirmap and ovw. Do not change a symbol's symbol type.

Submap Modifications

Submap modifications are made through the Modify→Describe Submap menu function.

You can change the "Comments" and the "Background Graphics" fields.

Changing the "Submap Name" is not recommended because, like the symbol label, the submap name is set by nrdlmap, and nrdlmap will override your customization when the user interface is shut down and brought back up.

Searching for Symbols

HP OpenView and IBM NetView for AIX provide fairly powerful search utilities. These search utilities can be used to locate symbols that match certain criteria. The following three search functions might be useful when searching for alarm symbols:

- Locate by Object Attribute
- Locate by Symbol Type
- Locate by Symbol Status

To use the Locate function, simply choose **Locate→Objects** from the main menu, and then pick the type of search you want.

For example, to view the number of unresolved **String Matches**, you could search by Symbol Type, and select the **Alarm:Content** symbol type. To determine how many critical elements you have in your network, you could do a search by Symbol Status, and then search for Critical (red) elements. Finally, to search for an alarm from a particular source IP address, you could search by Attribute, and then pick "Source IP Address" from the list of attributes, and then type in the source IP address you want to find.

Setting the Home Submap

When you start up the user interface, a submap that is designated the "home submap" is opened. By default, the root (top) level submap is the home submap. You may want to change the home submap to the child submap of the top level NSX Collection (the submap you get when you double-click on the NSX Collection that appears on the root level submap). If you want to make this change, perform the following steps:

1. **Double-click the** NetRanger **icon.**
2. **Select the menu option** Map→Submaps→Set This Submap As Home.

Changing a Submap Background

It is sometimes helpful to place a background picture on a submap to help identify the submap quickly. Submap backgrounds can also be used to help provide context for the different symbols on the submap (for instance, machine icons positioned strategically on a picture of a floor plan could help mark where the machines reside physically).

To add a submap background, open the submap that you want to change, and then select the menu option **Map→Submaps→Describe/Modify**. Under the **Background Graphics:** heading, press the **Browse...** button. From the pop-up list, select the background graphic of your choice. "usastates.gif" is a popular choice. You could also create a custom GIF file with any graphics program, and use that GIF file as an OpenView submap background. Press **OK** and then press **OK** again.

Repositioning Symbols on a Submap

You can use the mouse pointer to move symbols to different positions on a submap. However, if symbols are added to or removed from the submap, the user interface will automatically reposition *all* of the symbols on the submap, and the customization will be lost.

To prevent this, it is usually best to turn **automatic layout** off. To do this, choose **View→Automatic Layout**, and select the **off** option for either the current submap (if you are only repositioning symbols on a small subset of submaps) or for all submaps (if you reposition symbols frequently).

Hiding Symbols

Under some circumstances, you might want to prevent a symbol from appearing on a given submap, but you might not want, or be able, to delete the symbol. For instance, there could be a machine in a collection that you don't care about, but you can't delete it because it has unresolved alarms. Assume for the moment that there is some reason why you don't want to delete the alarms. In a situation like this, it is best to *hide* the symbols.

To hide a symbol, select it, then choose the menu option **Edit→Hide Object(s)**. You are given a choice of hiding **This Submap** or **All Submaps**. Pick the option of your choice.

To "unhide" a symbol, simply select the **Edit→Show Hidden Objects** menu function.

Changing the Status Propagation Schemes

When a symbol has Compound Status Source, the status (color) of the symbol is based solely on the status of the symbol(s) in that symbol's child submap. HP OpenView and IBM NetView for AIX provide the user with user-selectable sets of "rules" that the User Interface uses to determine the status of a symbol based on the status of the symbols in the child submap. These "rulesets" are called **Compound Status Source Propagation Schemes**, and the ruleset you choose will affect the color of the icons on the map.

To change the status propagation scheme, choose the **Map→Maps→Describe/Modify** menu option, select one of the radio buttons associated with a scheme, and then press **OK**.

WheelGroup Corporation highly recommends that you select the Propagate Most Critical scheme.

Consult the documentation provided with your network management platform for more information about Compound Status Source.

Changing Appearances, Fonts, Window Sizes, Colors, Etc.

In HP OpenView and IBM NetView for AIX there are special ASCII files called **Application Default** files that contain parameters that can be customized to change the look and feel of certain applications. To change fonts, window sizes, colors, etc. for the user interface in general, edit the OVw file which is in `$APP_DEFS` on HP systems and /usr/OV/app-defaults on IBM systems.

To modify the attributes of the various XNm applications, modify the XNm* files. The **Show Current Events** window uses an application called **xnmappmon** (X-Node Manager Application Monitor) to display data. If you want to change the appearance of this window, make the necessary modifications to this file.

Creating and Using Multiple Maps

The NetRanger Director supports the use of multiple OpenView Windows (ovw) maps. Using multiple maps in OpenView can be a little tricky, so consider reading the appropriate OpenView documentation before creating multiple maps.

Here are some things to remember about multiple maps:

- To delete an object from the object database, you must delete the object's symbols from all maps. For example, if an alarm object is represented on two different maps, the alarm must be deleted from both maps before the alarm is cleared from the object database.
- You can create customized maps for different users. Each user's map can have a different subset of NSX Machines displayed. This is helpful when trying to distribute responsibility for different NSX machines to different users.

To create a customized map for a user, either use the **Map→Maps→New** function or use the -m command line parameter when invoking ovw (see the appropriate OpenView documentation for details). When the new map is created, nrdirmap will represent all of the objects in the database on the new map. Once the new map has stopped Synchronizing, you can use the **Edit→Delete** function to remove the symbols that you don't want to be represented on that map.